PCSRF: Threats

- Attack mode
  - Physical
  - Cyber
  - Combined
- Undesired activity (including “acts of God”)
  - Access to restricted information
  - Interference with authorized operation
  - Unauthorized action
  - Inappropriate authorized action

PCSRF: Threat - undesired activity (1)

- Access to restricted information
  - Can give competitors an advantage
  - Fodder for opportunistic opponents: lawyers, environmentalists, …
  - Can assist implementation of other classes of attack
  - Can reduce detectability of other classes of attack
- Interference with authorized operation
  - Damage to physical plant (environmental impact, restoral cost and time and effort, loss of business)
  - Interference with meeting legal and/or contractual obligations
  - Impact on profits and customer satisfaction
  - Impact on stock price and credit rating
  - Impact on larger social group

PCSRF: Threat - undesired activity (2)

- Unauthorized action
  - Damage to plant and/or product
  - Theft or other loss of resources or inventory
  - Consequential damage to neighbors or customers and/or customers’ plant
- Inappropriate authorized action
  - Same as for unauthorized action
  - Permitted action exercised within inappropriate context
  - Aggregation of permitted actions leading to an impermissible result

PCSRF: System structure

- Within a geographic site:
  - Functional units of the physical plant
  - Cyber-connected sensors, actuators and control elements
  - Intra-site communications elements
  - Limited physical protection of the site
- Connections between geographic sites:
  - Inter-site physical interactions (e.g., pipe and fluid)
  - Inter-site communications elements
  - Minimal or no physical protection of the interconnections between sites

PCSRF: Cyber-protection

- Secrecy/confidentiality
  - Duration of required secrecy:
    - Short-term: deny attackers knowledge of system state
    - Medium-term: deny attackers knowledge of inventory levels during period of relevancy
    - Long-term: keep trade secrets
    - Variable: manage crypto parameters (duration a function of what the crypto protects)
  - Proposed countermeasures to attack:
    - Encrypt all such information using a symmetric secret key before it exits the physically protected environment
    - Key-strength determined by duration of secrecy requirement
    - Protection against quantum-computer-based cryptanalysis requires squaring key strength (≈ doubling key length)

PCSRF: Cyber-protection

- Integrity
  - Amount of required integrity:
    - Small: probability of not detecting alteration < 10^{-2}
    - Medium: probability of not detecting alteration < 10^{-4}
    - Large: probability of not detecting alteration < 10^{-2N}
  - Proposed countermeasures to attack:
    - Small: ≥ 7 bits of predictable value at end of message
    - Medium: ≥ 14 bits of predictable value at end of message
    - Large: ≥ 7N bits of predictable value at end of message
  - Proposed approach:
    - Forward chaining through message; integrity info at end
    - Point-to-(multi)point single source sessions: 0xF…F, or N-byte session message sequence number MOD $10^{2 \text{ or } 4 \text{ or } 2N}$, or successor message sequence number MOD $10^{2 \text{ or } 4 \text{ or } 2N}$
    - Multicast multi-source sessions: N-byte 0xF…F

PCSRF: Cyber-protection

- Authentication
  - Degree of required authentication:
    - Normal operational action: modest
    - Abnormal operational action: strong, typically 2-ϕ: enable message followed by trigger message within a time window
    - Configuration action (including software upgrade): strong, typically requires off-process state
    - Key management action: strong
  - Proposed countermeasures to attack:
    - Based partially on RFC3097
    - Protected against replay by advancing sequence numbers
    - Pairwise authentication via use of a pairwise-shared symmetric secret key, concurrent with integrity provided by the same pairwise-shared key
    - Multipoint authentication using either
      - An asymmetric private key encrypting a cryptographically strong message digest, where the recipients all have the corresponding public key, or
      - A series of pairwise-shared identified symmetric secret keys, one per recipient, encrypting a cryptographically strong message digest

PCSRF: Cyber-protection

- Non-repudiation
  - Degree of required non-repudiation:
    - No known need within machine – machine control networks
  - Proposed countermeasures to attack:
    - None required, due to lack of need for feature